MULTI-MODULE ENCRYPTION METHOD

Field of the invention

The present invention relates to the domain of the encipherment, or encryption, and the decipherment or decryption of data, and particularly of data, which is to remain inaccessible to unauthorized persons or appliances within the framework of pay-per-view television systems. In such systems, the data are enciphered in a secure environment, which accommodates considerable computational power, and is called the encoding subsystem. The data are then sent, by known means, to at least one decentralized subsystem where they are deciphered, generally by means of an IRD (Integrated Receiver Decoder) and with the aid of a chip card. A possibly unauthorized person can gain unrestricted access to this chip card and the decentralized subsystem, which cooperates with it.

Background of the invention

It is known practice to chain together various encryption/decryption means in an enciphering/deciphering system. In all of what follows, the expression encryption/decryption will be used to refer to a particular encryption means used in a bigger enciphering/deciphering system.

It has long been sought to optimize the operation of these systems from the triple viewpoint of speed, memory space occupied and security. Speed is understood to mean the time required to decipher the data received.

Encryption/decryption systems with symmetric keys are known. Their inherent security can be gauged as a function of several criteria.

The first criterion is that of physical security, relating to the ease or to the difficulty of a method of investigation by extracting certain components, this being followed by their possible replacement by other components. These replacement components, intended to inform the unauthorized person about the nature and manner of operation of the enciphering/deciphering system, are chosen by him/her in such a way as not to be detected, or to be as undetectable as possible, by the remainder of the system.

A second criterion is that of system security, within the framework of which attacks are not intrusive from the physical viewpoint but call upon analysis of mathematical type. Typically, these attacks will be conducted by computers of high power, which will attempt to break the algorithms and the enciphering codes.

Means of encryption/decryption with symmetric keys are for example the systems referred to as DES (Data Encryption Standard). These relatively old means now merely offer system security and physical security which are entirely relative. It is for this reason in particular that increasingly, DES, the lengths of whose keys are too small to satisfy the conditions of system security, is being replaced by new means of encryption/decryption or with longer keys. Generally, these means having symmetric keys call upon algorithms comprising enciphering rounds.

Other attack strategies are referred to as Simple Power Analysis and Timing Analysis. In Simple Power Analysis, one uses the fact that a microprocessor tasked with encrypting or decrypting data is connected to a voltage source (in general 5 volts). When it is idle, a fixed current of magnitude i flows through it. When it is active, the instantaneous magnitude i is dependent, not only on the incoming data, but also on the encryption algorithm. Simple Power Analysis consists in measuring the current i as a function of time. The type of algorithm, which the microprocessor is performing can be deduced from this.

In the same way, the method of Timing Analysis consists in measuring the duration of computation as a function of a sample presented to the decryption module. Thus, the relationship between the sample presented and the time for computing the result makes it possible to retrieve the decryption module secret parameters such as the key. Such a system is described for example in the document «Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems» published by Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisco, CA-USA.

To improve the security of the enciphering system, algorithms having asymmetric keys have been proposed, such as the so-called RSA (Rivest, Shamir and Adleman) systems. These systems comprise the generation of a pair of matched keys, one the so-called public key serving in the enciphering, and the other the so-called private key serving in the deciphering. These algorithms exhibit a high level of security, both system and physical security. They are on the other hand slower than the traditional systems, especially at the enciphering stage.

The most recent attack techniques call upon the so-called DPA concept, standing for Differential Power Analysis. These methods are based on suppositions, verifiable after a large number of trials, about the presence of a 0 or a 1 in a given position of the enciphering key. They are almost non-destructive, thus rendering them largely undetectable, and call upon both a physical intrusion component and a mathematical analysis component. Their manner of operation recalls the techniques for investigating oil fields, where an explosion of known power is generated at the surface and where earphones and probes, placed at likewise known distances from the site of the explosion, enable assumptions to be made about the stratigraphic composition of the subsurface without having to carry out too much digging, by virtue of the reflecting of the shock waves by the boundaries of sedimentary beds in this subsurface. DPA attacks are described in particular in § 2.1. of the document «A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards», published on 1st February 1999 by Suresh Chari, Charanjit Jutla, Josyula R. Rao and Pankaj Rohatgi, of IBM T. J. Watson Research Center, Yorktown Heights, NY.

The requirement of having to resist DPA attacks forces the use of so-called «whitening» jamming systems, either in the input information, or at the output of an enciphering/deciphering algorithm. The technique of whitening is described in § 3.5 of the same aforesaid document.

Moreover, the fact that the computation powers are limited in the decentralized subsystem of a pay-per-view television system creates a problem, which has never yet been satisfactorily solved, for performing the chaining described previously to a sufficient extent.

Summary of the invention

The objective of the present invention is to make available an encryption/decryption method which is resistant to modern methods of investigation such as described above.

This objective is achieved by a method of encryption and decryption carried out by a plurality of encryption/decryption modules arranged in series, wherein an encryption/decryption module, different from the first module, starts encryption/decryption operations as soon as said module receives a part of the results of encryption/decryption operations from the immediately preceding encryption/decryption module.

The particular feature of the method lies in the fact that an intermediate module does not start up when the result from the previous (or upstream) module has terminated but begins as soon as already part of the information is available. Therefore, for an outside observer, it is not possible to establish the input or output conditions for this module.

Since the deciphering occurs in the decentralized subsystem cooperating with the chip card, this chip card accommodating only relatively limited computational powers as compared with the encoding subsystem, it is for example beneficial to use a public asymmetric key, operating relatively fast, during the last steps of the deciphering. This makes it possible on the one hand to preserve the invulnerability characteristics of the system on exiting the procedure, and on the other hand to concentrate the computational power, related essentially to encipherment with the aid of the private key, in the encoding subsystem.

It has been discovered that extra security is afforded by the possibility of concatenating, or of partially interleaving, two means of encryption/decryption which follow one another sequentially. This concatenation or partial interleaving is understood to mean the process consisting in starting the action of the second encryption/decryption means on the data at a moment when the first encryption/decryption means has not yet terminated its work on these same data. This makes it possible to mask the data such as they would result from the work of the first module and before they are subjected to the action of the second module.

The chaining can start as soon as data computed at the output of the first module are partially available for processing by the second module.

The invention makes it possible to guard against the aforesaid attacks by combining various means of encryption/decryption in an enciphering/deciphering system, and possibly by associating concatenation or partial interleaving with the sequence in which these means follow one another.

Brief description of the drawings

The present invention will be understood in greater detail by virtue of the following drawings, taken by way of non-limiting example, in which:

- Figure 1 represents the encryption operations
- Figure 2 represents the decryption operations
- Figure 3 represents an alternative to the encryption method.

Detailed description of the invention

In a particular embodiment of the invention, the enciphering/deciphering system comprises an encoding subsystem where three algorithms are used sequentially:

a) an asymmetric algorithm A1 with private key d1. This algorithm A1 performs a signature on plain data, represented by a message m, this operation delivering a first cryptogram c1, by means of mathematical operations which are generally denoted in the profession by the formula: c1 = m exponent d1, modulo n1. In this formula, n1 forms part of the public key of the asymmetric algorithm A1, modulo represents the well-known mathematical operator of congruencies within the set of relative integers, and d1 is the private key of the algorithm A.

b) a symmetric algorithm S using a secret key K. This algorithm converts the cryptogram c1 into a cryptogram c2.

c) an asymmetric algorithm A2 with private key d2. This algorithm A2 converts the cryptogram c2 into a cryptogram c3, by means of the mathematical operation denoted, as previously, by: c3 = c2 exponent d2 mod n2, in which formula n2 forms part of the public key of the asymmetric algorithm A2, and d2 is the private key of the algorithm A2.

The cryptogram c3 leaves the encoding subsystem and arrives at the decentralized subsystem by means known per se. In the case of pay-per-view television systems, this may equally involve video data or messages.

The decentralized subsystem uses, in the order reverse to the above, three algorithms A1', S' and A2'. These three algorithms form part of three encryption/decryption means A1-A1', S-S' and A2-A2', distributed between the encoding subsystem and the decentralized subsystem, and representing the encryption/decryption system.

d) the algorithm A2' performs a mathematical operation on c3 which restores c2 and is denoted: c2 = c3 exponent e2 mod n2. In this formula, the set consisting of e2 and n2 is the public key of the asymmetric algorithm A2-A2'.

e) the symmetric algorithm S' using the secret key K restores the cryptogram c1.

f) the asymmetric algorithm A1' with public key e1, n1 retrieves m by performing the mathematical operation denoted: m = c1 exponent e1 mod n1.

The concatenation, in the decentralized subsystem, consists in starting the decoding step e) whilst c2 has not yet been completely restored by the previous step d), and in starting the decoding step f) whilst c1 has not been completely restored by step e. The advantage is to thwart an attack aimed for example firstly at extracting, within the decentralized subsystem, the cryptogram c1 at the end of step e, so as to compare it with the plain data m, then by means of c1 and of m to attack the algorithm A1', and then gradually to backtrack up the coding chain.

The concatenation is not necessary in the encoding subsystem, which is installed in a secure physical environment. It is on the other hand useful in the decentralized subsystem. In the case of pay-per-view television, the IRD is in fact installed at the subscriber's premises and may be the subject of attacks of the pre-described type.

It will be appreciated that an attack of a combination of three concatenated decryption algorithms A1', S' and A2' has much less chance of succeeding than if the cryptograms c1 and c2 are fully reconstructed between each step d), e) and f). Moreover, the fact that the algorithms A1' and A2' are used with public keys e1, n1 and e2, n2 implies that the means of computation required in the decentralized subsystem are much reduced as compared with those in the encoding subsystem.

By way of example and to fix matters, steps a) and c), that is to say the encryption steps with private keys, are 20 times longer than the decryption steps d) and f) with public keys.

In a particular embodiment of the invention, derived from the previous one, the algorithms A1 and A2 are identical as are their counterparts A1' and A2'.

In a particular embodiment of the invention, also derived from the previous one, in step c) the public key e2, n2 of the asymmetric algorithm A2 is used whilst in step d) the cryptogram c3 is decrypted with the private key d2 of this algorithm. This embodiment constitutes a possible alternative when the resources of the decentralized subsystem in terms of computational power are far from being attained.

Although chip cards are used chiefly for decrypting data, there are also chip cards having the capacities required to perform encryption operations. In this case, the attacks described above will pertain also to these encryption cards which operate away from protected locations such as a management center. This is why the method according to the invention applies also to serial encryption operations, that is to say that the downstream module begins its encryption operation as soon as part of the information delivered by the upstream module is available. This process has the advantage of interleaving the various encryption modules, and as a consequence the result from the upstream module is not completely available at a given time. Moreover, the downstream module does not begin its operations with a complete result but on parts, thereby making it impracticable to interpret the manner of operation of a module with respect to a known input state or output state.

In Figure 1, a data set m is introduced into the encryption chain. A first element A1 performs an encryption operation using the so-called private key, composed of the exponent d1 and of the modulo n1. The result of this operation is represented by C1.. According to the mode of operation of the invention, as soon as part of the result C1 is available, the next module begins its operation. This next module S performs its encryption operation with a secret key. As soon as it is partially available the result C2 is transmitted to the module A2 for the third encryption operation using the so-called private key composed of the exponent d2 and of the modulo n2. The final result, here dubbed C3, is ready to be transmitted by known pathways such as over the airwaves or by cable.

Figure 2 represents the decryption system composed of the three decryption modules A1' S', A2' which are similar to those which served for encryption, but are ordered in reverse. Thus, one commences firstly with the module A2' which performs its decryption operation on the basis of the so-called public key composed of the exponent e2 and of the modulo n2. In the same way as for encryption, as soon as part of the result C2 from the module A2' is available, it is transmitted to the module

S' for the second decryption operation. To terminate decryption, the module A1' performs its operation on the basis of the so-called public key composed of the exponent e1 and of the modulo n1.

In a particular embodiment of the invention, the keys of the two modules A1 and A2 are identical, that is to say that on the encryption side, d1 = d2 and n1 = n2. By analogy, during decryption, e1 = e2 and n1 = n2. In this case, one speaks of the private key d, n and of the public key e, n.

In another embodiment of the invention, as illustrated in Figures 3 and 4, the module A2 uses the so-called public key instead of the so-called private key. At the moment of encryption, the public key e2, n2 is used by the module A2, (see Figure 3) and during decryption (see Figure 4), the module A2' uses the private key d2, n2 to operate. Although this configuration exhibits an overhead of work for the decryption set, the use of a private key reinforces the security offered by the module A2.

The example illustrated in Figures 3 and 4 is not restrictive in respect of other combinations. For example, it is possible to configure the module A1 so that it performs the encryption operation with the public key and the decryption with the private key.

It is also possible to replace the encryption/decryption module having secret key S with a module of the type with asymmetric keys of the same type as the modules A1 and A2.